97. (NEW) A protected processing environment comprising:

means for providing a tamper resistant enclosure;

means for maintaining at least one public verification key within the tamper resistant enclosure; and

means for authenticating load modules based, at least in part, on use of the public verification key.

98. (NEW) A method of distinguishing between trusted and untrusted load modules comprising:

(a) receiving a load module,

(b) determining whether the load module has an associated digital signature,

(c) if the load module has an associated digital signature, authenticating the digital signature using at least one secret public key; and

(d) conditionally executing the load module based at least in part on the results of authenticating step (c).

99. (NEW) A method of increasing the security of a virtual distribution environment comprising plural interoperable protected processing environments having different work factors, the method comprising:

(a) classifying the plural protected processing environments based on work factor,

(b) distributing different verification public keys to different protected processing environments having different work factor classifications, and

(c) using the distributed verification public keys to authenticate load modules, including the step of preventing protected processing environments having different work factor classifications from executing the same load module.

100. (NEW) A protected processing environment, comprising:

a tamper resistant barrier having a first work factor; and

at least one arrangement within the tamper resistant barrier that prevents the protected processing environment from executing the same load module accessed by a further protected processing environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

101. (NEW) A method for protecting a computation environment surrounded by a tamper resistant barrier having a first work factor, the method including:

preventing the computation environment from using the same software module accessible by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

102. (NEW) A method of protecting computation environments comprising:

(a) associating plural digital signatures with a load module;

(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and

(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.

C1

103. (NEW) A computer security method comprising:

digitally signing, using a first digital signing technique, a first executable designating the first executable for use by a first device class; and

digitally signing, using a second digital signing technique different from the first digital signing technique, a second executable designating the second executable for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class.

104. (NEW) A method of authenticating an executable comprising:

(a) authenticating a first digital signature associated with the executable, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and

(b) authenticating a second digital signature associated with the executable, including the step of employing at least one of:

(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,

(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and

(iii) a second public key that is dissimilar to the first public key.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

105. (NEW) A secure execution space comprising:

means for providing a tamper resistant barrier;

means for maintaining at least one public verification key within the tamper resistant barrier; and

means for authenticating executables based, at least in part, on use of the public verification key.

106. (NEW) A method of distinguishing between trusted and untrusted executables comprising:

(a) receiving an executable;

(b) determining whether the executable has an associated digital signature;

(c) if the executable has an associated digital signature, authenticating the digital signature using at least one secret public key; and

(d) conditionally executing the executable based at least in part on the results of authenticating step (c).

107. (NEW) A method of increasing the security of plural interoperable secure execution spaces having different work factors, the method comprising:

(a) classifying the plural secure execution spaces based on work factor;

(b) distributing different verification public keys to different secure execution spaces having different work factor classifications; and

(c) using the distributed verification public keys to authenticate executables, including the step of preventing secure execution spaces having different work factor classifications from executing the same executable.

108. (NEW) A protected processing environment comprising:

a tamper resistant barrier having a first work factor; and

at least one arrangement within the tamper resistant barrier that prevents the secure execution space from executing the same executable accessed by a further secure execution space having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

109. (NEW) A method for protecting a computation environment surrounded by a tamper resistant barrier having a first work factor, the method including:

preventing the computation environment from using the same software module accessed by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

C1

110. (NEW) A method of protecting computation environments comprising:

(a) associating plural digital signatures with an executable;

(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and

(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049